JOINT ESA-NASA SPACE FLIGHT SAFETY CONFERENCE

"Safety Through Partnership"

June 11-14, 2002

ESTEC, Noordwijk, The Netherlands

SESSION IV.3 PAYLOAD SAFETY– Part 3:

Mechanical Systems

Presentation Overview

- Requirements and Interpretation Letters
- Overview of Mechanical Systems Safety Interpretation Letter
- Design and Verification Provisions
- Mechanical Systems Verification Plan

Requirements and Interpretation letters

- Payload Safety Requirements NHB/NSTS 1700.7B
- NSTS 14046 Rev. E Payload Verification Requirements
- Mechanical System Safety Interpretation Letter JSC, MA2-00-057 (Sept 28, 2000)

Mechanical System Safety

Interpretation Letter Overview

- Consolidation and clarification of safety requirements for the design and verification of mechanisms (movable mechanical systems) used in safety critical applications
- Addresses assurance of safety critical functionality for mechanical systems
  - Ability to operate or the ability to retain configuration
  - Not intended to address their strength as a structural element
  - Not intended to address the electrical aspects of an electromechanical system
- "Safety Critical" refers to a system which has the potential to result in a critical or catastrophic hazard if failed

Mechanical System Safety

Interpretation Letter Overview

- Provides clarification on usage of the "design for minimum risk" (DFMR) approach as it applies to functionality of a movable mechanical system

- Specifies that compliance with DFMR criteria can normally be used to establish safety compliance
  - Designs with only one additional control or backup for a catastrophic hazard
  - Without additional controls for a critical level hazard

- Also permits the use of fully compliant "simple" mechanical systems without mechanical redundancy
  - DFMR "simple" mechanisms can be considered as having two-failure-tolerance equivalency, when specifically approved by the PSRP/SRP.
  - A simple mechanical system is defined as a robust mechanism that has relatively few moving parts and can demonstrate low sensitivity to environmental and operational conditions

Mechanical System Safety

Interpretation Letter Overview

- A design can be considered to meet DFMR in functionality if it can be demonstrated that credible failure modes have been eliminated
- Failure modes that must be considered for credibility include, but are not limited to binding, jamming, inadvertent operation, failure to function, etc
- The DFMR approach must include design implementation and verification provisions outlined in items 1 through 11 of the interpretation letter, unless its clearly not applicable.
  - Alternate approaches to the design, build, and test provisions may be accepted based on a clearly substantiated safety equivalency
- These items will be topics of the payload safety review process for all safety critical mechanical systems
- Mechanical Systems Working Group (MSWG) assesses compliance to safety requirements and the interpretation letter

Mechanical System Safety

Interpretation Letter Overview

1.0 Binding/Jamming/Seizing

- Designs shall include provisions to prevent binding/jamming/seizing
- Appropriate design provisions include, but are not limited to:
  - Dual rotating surfaces or other mechanical redundancies
  - Robust strength margins such that self-generated internal particles are precluded
  - Shrouding and debris shielding,
  - Proper selection of materials and lubrication design to prevent friction welding or galling
- Designs shall also establish dimensional tolerances on all moving parts to ensure proper functional performance
  - Must consider all natural and induced environmental conditions
    - thermally induced in-plane and out of plane distortions
    - differential thermal growth and shrinkage
    - load induced deflections
  - Must take into account tolerances associated with rigging (mechanical adjustment)

Mechanical System Safety

Interpretation Letter Overview

1.0 Binding/Jamming/Seizing (continued)

- Designs shall ensure compatibility of any lubricants
  - Compatibility with interfacing materials and other lubricants used in the design,
  - Compatibility with the natural and induced environment.
  - The design shall also address proper quantities of lubricant.

Mechanical System Safety

Interpretation Letter Overview

2.0 Quick Release Pins

- Quick release pins (push-in-place (pip)-pins) are considered movable mechanical systems
- A pip-pin design qualified by inspection and test to the provisions of MIL-P-23460, or equivalent, shall be used in any system design incorporating pip-pins
- All flight pip-pins shall be subjected to environmental acceptance testing
- Pip-pins shall undergo qualification vibration test
  - In place in their respective hardware locations during the qualification test of the total assembly
  - Or, component test to the predicted qualification levels at the hardware location
- Pip-pins shall also be subjected to thermal qualification testing to the max/min flight temperatures
- Due to a history of failures with pip-pins, the "simple" mechanical system approach is not applicable

Mechanical System Safety

Interpretation Letter Overview

3.0 Springs

- Safety critical springs shall be redundant or designed, evaluated, and used under an acceptable fracture control program (ref. NASA-STD-5003)

- Failure of springs that are properly controlled under an acceptable fracture control program is considered non-credible

- The design and use of a fail-safe spring or the use of a spring that maintains functionality with the loss of a single coil is acceptable

- Compression springs should be used in lieu of tension or torsional springs, where practical

Mechanical System Safety

Interpretation Letter Overview

4.0 Fastener Retention

- A means of positive locking (i.e., self-locking threads, self-locking inserts, etc.) shall be provided on all fasteners (threaded and otherwise)

- Assures integrity of the mechanical assemblies and prevents loose parts.

- Positive locking is in addition to the standard torque/preload of the fastener

- Locking compounds shall not be used on fasteners to provide locking, where other positive locking methods are practicable

Mechanical System Safety

Interpretation Letter Overview

5.0 Strength and Fracture Control

- Structural design of safety critical mechanical system components shall adhere to paragraphs 208.1, 208.2, and 208.3 of NSTS 1700.7
- Movable mechanical assemblies used in safety critical applications shall be included in an acceptable fracture control program (ref. NASA-STD-5003)
- Components and linkages shall be designed with sufficient strength to tolerate an actuation force/torque stall condition at any point of travel
- A positive margin of safety must be demonstrated with an ultimate factor of safety applied
- End of travel mechanical stops shall be designed to have positive strength margins for worst case dynamic loading conditions
  - Must consider variables in inertia properties, actuation force/torque, drive train resistance, and other environmental conditions

Mechanical System Safety

Interpretation Letter Overview

5.0 Strength and Fracture Control (continued)

- Exposed mechanical system components, protective shrouds and covers, and mounting structure shall be designed to accommodate inadvertent impact loads

- RMS/SSRMS/payload operations
  - EVA/IVA loads
  - Must ensure adequate margins to preclude deformation that could cause a binding or jamming condition or inadvertent operation of the mechanism

- A design that incorporates preload as a means of meeting functional and/or structural requirements shall comply with the preload criteria defined in NSTS 08307

Mechanical System Safety

Interpretation Letter Overview

6.0 Positive Indication of Status

- All movable mechanical systems shall provide positive indication that the mechanism has achieved its desired position (i.e., "ready-to-latch," "latched").

- End of travel stops shall be provided for all safety critical movable mechanical systems.

Mechanical System Safety

Interpretation Letter Overview

7.0 Torque/Force Margins

- The margin is the mechanism's torque or force available to perform a function over and above the torque or force actually necessary to perform a function
- Margin, as demonstrated conservatively by test or analytical calculations, shall take into account the following worst case environmental conditions including:
  - Frictional effects
  - Alignment effects
  - Latching forces
  - Thermally induced distortions
  - Load induced distortions
  - Variations in lubricity including degradation or depletion of lubrication under vacuum and under worst case thermal conditions
- Operating Torque Margin = (Available Driving Torque/Resistive Torque) -1
  - For linear devices, "Force" replaces "Torque" in the above equation

Mechanical System Safety

Interpretation Letter Overview

7.0 Torque/Force Margins (continued)

- The holding torque or force margin is the margin provided to prevent inadvertent operation
- Margin, as conservatively demonstrated by test or analytical calculations, shall take into account worst case environmental conditions that work against the holding force/torque including:
  - Frictional effects
  - Alignment effects
  - Latching forces
  - Thermally induced distortions
  - Load induced distortions
  - Inertial Loading of Mechanical Components
- Holding Torque Margin = (Available Holding Torque/Torque Applied by Limit load) -1
  - For linear devices, "Force" replaces "Torque" in the above equation

Mechanical System Safety

Interpretation Letter Overview

7.0 Torque/Force Margins (continued)

- Both operating and holding torque/force margins shall be acceptance-test verified unless another verification approach is approved by the MSWG
- A margin of 1.0 or greater is required at every point of travel when test verified
  - Test verification of the amount of driving or holding torque or force available under conservative adverse conditions
  - Does not require a mechanical system demonstration at greater than limit load conditions
- Verification by analysis only will require prior review and approval of the analytical approach and margin requirement by the MSWG

Mechanical System Safety

Interpretation Letter Overview

8.0 Contamination

- Fabrication and handling of safety critical movable mechanical assemblies shall be accomplished in a clean environment
  - Avoidance of non-particulate (chemical) as well as particulate air contamination
  - The particulate cleanliness of internal moving subassemblies shall be maintained to at least level 500 as defined in MIL-STD-1246

- Specific cleanliness requirements shall be established for each movable mechanical assembly
  - Shall address cleanliness levels needed to prevent binding or jamming

Mechanical System Safety

Interpretation Letter Overview

9.0 Assembly Level Acceptance Tests

- Each flight and qualification test article shall be subjected to acceptance testing
  - Run-in
  - Functional
  - Environmental testing
- The acceptance tests shall be structured to detect workmanship defects that could affect operational performance
- 9.1 Run-in Test:
  - Run-in test shall be performed on each movable mechanical assembly after initial functional testing before it is subjected to further acceptance testing
  - Objective is to detect any material/workmanship defects and to wear-in parts to ensure consistent and stable operation

Mechanical System Safety

Interpretation Letter Overview

9.0 Assembly Level Acceptance Tests (continued)

- 9.2 Functional and Environmental Acceptance Tests:
  - Each movable mechanical assembly shall be subjected to functional and environmental tests
  - Functional tests shall be structured to demonstrate that the movable mechanical assembly is capable of operating to satisfy all performance requirements
  - Functional tests are required before and after exposure to environmental test conditions in order to establish whether damage or degradation in performance has occurred
  - Environmental acceptance tests shall be structured to demonstrate the ability to achieve performance requirements when exposed to the expected environmental extremes and to identify any workmanship defects

Mechanical System Safety

Interpretation Letter Overview

10.0 Qualification Test

- A Qualification Test Program (QTP) shall be established for each safety critical movable mechanical assembly
- A QTP shall assure that the mechanism design performance and safety margin exists with respect to safety critical functions (must work and/or must not work)
- Verification of all design requirements when exposed to any mechanical, electrical, environmental, or operational conditions
- Mechanism shall be tested in the launch, on-orbit and landing configurations
- Mechanism must be exposed to the appropriate corresponding environmental extremes
- Mechanism must be in its appropriate corresponding passive or operating state
- Inspection and functional tests are required before and after qualification tests
- MIL-STD-1540D may be helpful in establishing an effective Qualification Test Program.
- Development testing prior to QTP is highly recommended to reduce costly redesign

Mechanical System Safety

Interpretation Letter Overview

11.0 Design Life Verification Test

- Design life verification testing shall be conducted to verify design life requirements in applications where design life sensitivity could exist
- Fatigue limits being exceeded due to highly loaded components
  - Potential for deterioration of lubrication
  - Excessive wear due to high contact stresses
- Design life testing for mechanisms that pose a catastrophic hazard potential shall assure at least four times the total number of required cycles including:
  - Total number of mission operational cycles
  - Total number of component and vehicle functional and environmental test cycles
- Design life testing for mechanisms that pose a critical hazard potential shall assure at least two times the total number of cycles including:
  - Total number of mission operational cycles
  - Total number of component and vehicle functional and environmental test cycles

Mechanical System Safety

Interpretation Letter Overview

11.0 Design Life Verification Test (continued)

- Inspection and functional tests are required before and after design life verification tests

- For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion

- Refurbishment shall be accomplished after the design life verification tests and prior to re-acceptance testing.

Mechanical System Safety

Interpretation Letter Overview

Mechanical Systems Verification Plan

- A comprehensive Mechanical Systems Verification Plan (MSVP) must be submitted for review and approval by the MSWG.
  - Must describe the design and verification approach for safety critical movable mechanical systems
  - If DFMR approach is to be used the MSVP must address each of the design and verification provisions outlined in the interpretation letter

- The specific purpose of this plan is to establish an understanding on how applicable systems requirements will be implemented and verified.

- Before a movable mechanical system can be classified as a DFMR Mechanical System, compliance to the subject letter requirements must be provided to and approved by the MSWG.

Mechanism holding torque or force margin shall be acceptance-test verified unless another verification approach is approved by the MSWG. When test verified, a margin of 1.0 or greater is required in the applicable mechanism holding configuration(s). The holding torque or force margin is the margin provided to prevent inadvertent operation. Verification by analysis only will require prior review and approval of the analytical approach and margin requirement by the MSWG. This margin, as conservatively demonstrated by test or analytical calculations, shall take into account worst case environmental conditions, frictional effects, alignment effects, latching forces, thermally induced distortions, and load induced distortions, etc. The holding torque margin is defined as:

$$\textit{Holding Torque Margin} = (\textit{Available Holding Torque} / \textit{Torque Applied by Limit Load}) - 1$$

For linear devices, "Force" replaces "Torque" in the above equation.

Verification by test, as specified in this paragraph, does not require a mechanical system demonstration at greater than limit load conditions but rather requires a test verification of the amount of driving or holding torque or force available under conservative adverse conditions.

8.0 Contamination. Fabrication and handling of safety critical movable mechanical assemblies shall be accomplished in a clean environment with attention given to avoiding nonparticulate (chemical) as well as particulate air contamination. Specific cleanliness requirements shall be established for each movable mechanical assembly and shall address cleanliness levels needed to prevent binding or jamming.

9.0 Assembly Level Acceptance Tests. Each movable mechanical assembly designated for flight or as a qualification test article shall be subjected to acceptance testing which incorporates run-in, functional, and environmental testing. The acceptance tests shall be structured to detect workmanship defects that could affect operational performance. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion.

9.1 Run-in Test. After initial functional testing, a run-in test shall be performed on each movable mechanical assembly before it is subjected to further acceptance testing. The purpose of the run-in test is to detect material/workmanship defects and to wear-in parts.

9.2 Functional and Environmental Acceptance Tests. Each movable mechanical assembly shall be subjected to functional and environmental tests. Functional tests shall be structured to demonstrate that the movable mechanical assembly is capable of operating to satisfy all performance requirements. Functional tests are required before and after exposure to environmental test conditions in order to establish whether damage or degradation in performance has occurred. Environmental acceptance tests shall be structured to demonstrate the ability to achieve performance requirements when exposed to the expected environmental extremes and to identify any workmanship defects.

10.0 Qualification Test. A Qualification Test Program shall be established for each safety critical movable mechanical assembly. The qualification test program shall assure that a design performance and safety margin exists with respect to all design requirements when exposed to any mechanical, electrical, environmental, including acceptance testing, and

operational stimuli that the product may reasonably expect to encounter during its service life. The mechanism shall be tested in its launch, on-orbit, and landing configurations with the appropriate corresponding environmental extremes and with the mechanism in its appropriate passive or operating state. Inspection and functional tests are required before and after qualification tests. MIL-STD-1540D may be helpful in establishing an effective Qualification Test Program. Natural and induced environmental conditions shall include but are not limited to, thermally induced in-plane and out-of-plane distortions, differential thermal growth and shrinkage, and load-induced deflections. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion.

11.0 Design Life Verification Tests. For applications where design life might be a concern due to endurance or fatigue limits being exceeded, potential deterioration of lubrication, or excessive wear, design life verification testing shall be conducted to verify that design life requirements have been complied with. Design life testing for mechanisms that pose a catastrophic hazard potential shall assure at least four times the number of operational cycles, plus four times the number of component and vehicle functional and environmental test cycles. Design life testing for mechanisms that pose a critical hazard potential shall assure at least two times the number of operational cycles, plus two times the number of component and vehicle functional and environmental test cycles. Inspection and functional tests are required before and after design life verification tests. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion. Refurbishment shall be accomplished after the design life verification tests and prior to reacceptance testing.

A comprehensive Mechanical Systems Verification Plan that describes the verification approach for safety critical movable mechanical systems must be submitted for review and approval by the MSWG. The specific purpose of this plan is to establish an understanding on how applicable systems requirements will be implemented and verified. Before a movable mechanical system can be classified as a DFMR Mechanical System, compliance to the subject letter requirements must be provided to and approved by the MSWG. Although cancelled, mechanical system designers may still refer to MIL-A-83577 as a guideline during the design and verification process. Questions concerning this letter should be directed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, JSC/NC4, at (281) 483-8848.

Original Signed By:

William H. Gerstenmaier

Original Signed By:

Jay H. Greene

Enclosure

cc:
See List

Distribution:
CB/G. D. Griffith
DO12/J. M. Childress
EA44/R. J. Wren
MA2/A. M. Larsen
MA2/D. E. O'Brien
MA2/D. W. Whittle
MA2/J. G. Williams
NC4/M. L. Ciancone
NC55/SAIC/E. J. Conner
NE2/G. L. Priest
OZ3/D. W. Hartman
SD2/M. E. Coleman
USA/USH-700D/H. A. Maltby

cc:
AE/J. F. Whiteley
CA/J. D. Wetherbee
CB/C. J. Precourt
DA/B. R. Stone
EA/L. S. Nicholson
EA4/D. A. Hamilton
KN/NASDA/T. Akutsu
LM/I. M. Dornell
MA/R. D. Dittemore
MG/R. H. Heselmeyer
MM/J. B. Costello
MM/T. W. Logan
MQ/M. D. Erminger
MS/L. D. Austin, Jr.
MS3/D. L. Ladrach
MS3/K. B. Packard
MT/R. M. Swalin
MV/R. R. Roe, Jr.
NC44/M. L. Mudd
OA/T. W. Holloway
OE/J. B. Holsomback
OI/W. J. Bennett
OR/CSA/H. L. Williams
OT/ESA/U. J. Thomas
XA/G. J. Harbaugh
HQ/M-4/W. M. Hawes
HQ/MO/S. R. Nichols
HQ/M-7/N. B. Starkey
KSC/EC-G1/J. C. Dollberg
KSC/MK/J. D. Halsell, Jr.
KSC/MK-SIO/R. L. Segert
USA/USH-700D/L. Lo

Canadian Space Agency
Space Station Program
Attn: P. M. Jean
Manager, Safety and Product Assurance
6767 route de l'Aeroport
Saint-Hebert, Quebec
Canada J3Y 8Y9

ESTEC-GPQ
Attn: T. Sgobba
T. Heimann
P. O. Box 299 NL
2200 AG, Noordwijk
The Netherlands

NASDA
Tsukuba Space Center
Attn: H. Hasegawa
Space Station Safety and Product
Assurance Office
Reliability Assurance
2-1-1 Sengen
Tsukuba-shi, Ibaraki
Japan 305

RSC Energia
Attn: P. Vorobiev
4a Lenin Street
Korolev
141070 Moscow Region
Russia